

CLAIMS:

What is claimed is:

1 1. A method in a computer system for generating a
2 certificate for use only within said computer system to
3 authenticate operations internal to said computer system,
4 said method comprising the steps of:

5 establishing a security subsystem within said computer
6 system;

 establishing a master key pair including a master
private key and a master public key;

 storing said master private key in a protected storage
within said security subsystem, wherein said master private
key is inaccessible outside of said security subsystem;

 supplying a target public key;

 requesting generation of a self-verifying certificate;

 prompting a user for an authentication code in response
to a request for generation of said certificate; and

 generating a self-verifying certificate utilizing said
target public key and said master key pair only in response
to a correct entry of said authentication code, said
certificate used only internally within said computer
system.

1 2. The method according to claim 1, further comprising the
2 step of storing said authentication code in said security
3 subsystem.

1 3. The method according to claim 2, further comprising the
2 step of prohibiting an alteration of said authentication
3 code after said authentication code is stored in said
4 security subsystem.

1 4. The method according to claim 2, further comprising the
2 step of prohibiting access to said authentication code to
3 devices outside of said security subsystem after said
4 authentication code is stored in said security subsystem.

1 5. The method according to claim 1, further comprising the
2 step of determining a certificate identifier after a correct
3 entry of said authentication code, said certificate
4 identifier uniquely identifying said certificate.

1 6. The method according to claim 1, further comprising the
2 steps of:

3 said security subsystem generating security data for
4 said certificate after a correct entry of said
5 authentication code;

6 said security subsystem hashing said security data;

7 said security subsystem encrypting said security data
8 utilizing said master private key to create a signature; and

9 said security subsystem appending said signature to
10 said security data to create said certificate.

1 7. The method according to claim 1, further comprising the
2 step of storing said certificate along with a certificate
3 identifier in said computer system.

4 8. The method according to claim 1, further comprising the
5 steps of

6 receiving information within an appended certificate;

7 requesting authentication of a signature included
8 within said appended certificate;

9 said security subsystem reading said master public key
10 from said protected storage;

11 said security subsystem using said master public key to
12 decrypt said signature; and

13 said security subsystem determining whether said
14 signature is authentic.

1 9. A computer system for generating a certificate for use
2 only within said computer system to authenticate operations
3 internal to said computer system, said method comprising the
4 steps of:

5 a security subsystem within said computer system;

6 a master key pair including a master private key and a
7 master public key;

8 a protected storage within said security subsystem for
9 storing said master private key, wherein said master private
10 key is inaccessible outside of said security subsystem;

11 a target public key;

12 said computer system including a CPU executing code for
13 requesting generation of a self-verifying certificate;

14 said computer system including a CPU executing code for
15 prompting a user for an authentication code in response to a
16 request for generation of said certificate; and

17 a self-verifying certificate generated utilizing said
18 target public key and said master key pair only in response
19 to a correct entry of said authentication code, said
20 certificate used only internally within said computer
21 system.

1 10. The system according to claim 9, further comprising
2 said security subsystem for storing said authentication
3 code.

1 11. The system according to claim 10, further comprising
2 said computer system including a CPU executing code for
3 prohibiting an alteration of said authentication code after
4 said authentication code is stored in said security
5 subsystem.

1 12. The system according to claim 10, further comprising
2 said computer system including a CPU executing code for
3 prohibiting access to said authentication code to devices
4 outside of said security subsystem after said authentication
5 code is stored in said security subsystem.

1 13. The system according to claim 9, further comprising a
2 certificate identifier being determined after a correct
3 entry of said authentication code, said certificate
4 identifier uniquely identifying said certificate.

1 14. The system according to claim 9, further comprising:

2 said security subsystem for generating security data
3 for said certificate after a correct entry of said
4 authentication code;

5 said security subsystem for hashing said security data;

6 said security subsystem for encrypting said security
7 data utilizing said master private key to create a
8 signature; and

9 said security subsystem for appending said signature to
10 said security data to create said certificate.

1 15. The system according to claim 9, further comprising
2 said certificate being stored along with a certificate
3 identifier in said computer system.

16. The system according to claim 9, further comprising:

 said computer system including a CPU executing code for
 receiving information within an appended certificate;

 said computer system including a CPU executing code for
 requesting authentication of a signature included within
 said appended certificate;

 said security subsystem for reading said master public
8 key from said protected storage;

9 said security subsystem for using said master public
10 key to decrypt said signature; and

11 said security subsystem for determining whether said
12 signature is authentic.